

# **EXHIBIT 27**



## Cyber Aware

---

# Better Protect Your Online Accounts with “Two-Factor Authentication”

share    

---

Two-Factor authentication adds an extra security layer to your accounts across the internet. Two-factor authentication (2FA) means your accounts require information beyond user name and password to confirm you are who you say you are before you can get into the accounts.

The “second factor” comes in after you enter your username and password, which are considered to be the “first factor.” 2FA can be used to confirm your identity by asking for an extra piece of information. The additional information can be:

Something you *know*, like an additional passcode.

Something you *have*, like your phone to receive a one-time authorization code.

Something you *are*, like a fingerprint or voice print. This is also called biometric security.

The idea is to provide another piece of information a hacker would not have, making it harder for the bad guy to break into your account. Think of it like this: two-factor authentication is the difference between putting your socks in a drawer and your jewelry in a locked safe. Both are reasonably secure closed spaces, but your socks are easier for anyone to get.

There are a variety of ways companies reach out to you to complete the two-factor authentication. Some common ways include:

**Text or Email PIN** — A unique and temporary Personal Identification Number or code is sent to you via text or email using the phone number or email address associated with the account.

**Phone Call** — This method calls the phone associated with the account and waits for you to pick up and follow the directions to confirm your identity.

**Push Notification** — A notification for your approval will appear on a personal device you assign to the account.

But two-factor authentication is not fool-proof. Bad guys can try to trick you into giving up your information by using social engineering. That's where they use a phone call or email and pretend to be someone they are not. You can learn more about social engineering [here](#). Make sure to keep your guard up and don't give out your information carelessly. If you believe a caller is trying to scam you, hang up. Call 611 and ask for the Fraud Department to report the call.

Also, if you change or give up your phone number, make sure to update all your accounts that use that number as a way to contact or authenticate you. It is important to take action before you lose access to the "old" number since it could be allocated to someone else in the future. If you don't, it's possible that the number's new owner could get your security messages in the future.

In the future, you can expect to see more organizations using 2FA, including possible biometric options, to help provide better security for customers. The Mobile Authentication Taskforce, comprised of AT&T and the three other major U.S. wireless carriers, continues to work on new multi-factor authentication solutions specifically designed to more easily, accurately and securely authenticate a user's online identity.

It's important to understand and embrace whatever security system a company uses. That added security is in place to protect you and your account.

*Take our [Cyber Aware quiz](#) to see how you score when it comes to protecting your accounts, devices and information.*

## More Blogs

[\\*Privacy Policy \(updated\)](#)    [Terms of Use](#)    [Accessibility](#)    [Contact Us](#)    [Subscribe to AT&T News](#)  
[Do Not Sell My Personal Information](#)

© 2021 AT&T Intellectual Property. All rights reserved.